UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,194	02/12/2002	Klimenty Vainstein	2222.5390003	7090

26111 7590 11/10/2008

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
11/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/075,194	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/23/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's submission for RCE filed on 08/27/2008 is entered. Applicant has amended claims 1, 2, 5-9, 12, 14, 21, 28, 34-36, 40-42 and 44. Currently claims 1-44 are pending in this application.

Response to Arguments

1. Applicant's arguments with respect to claims 1-44 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-19, and 21-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell et al. (WO 01/77783 A2), hereinafter, "Russell" in view of En-Seung et al. (US 6,892,306 B1), hereinafter, "En-Seung" and further in view of Richards et al. (US 2002/0016922 A1), hereinafter, "Richards".

Regarding Claims 1 and 34, Russell discloses method and corresponding computer program for providing access management through use of a plurality of server machines associated with different locations (see, Fig. 1), said method comprising the acts of:

(a) receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location (see, page 24, lines 2-7);

(b) authenticating a user of the first client machine at the first location (see, Page 11, lines 30-31);

(c) authenticating the first client machine (See, Page 25, lines 6-14);

(d) upon successful authentication in steps (b) and (c), retrieving at the first server machine access rules for the secured item (see, Page 25, lines 23-30);

(e) permitting access to the secure item via the first location when said authenticating (b) and (c) are successful, and further when allowed by the access rules (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13);

(f) permitting access to the secure item via the first server machine when said permitting (e) permits the user to gain access to the secure item from the first location (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13); and

(g) preventing access to the secure item via the first server machine when said permitting (e) does not permit the user to gain access to the secure item from the first location (see Page 26, lines 7-9).

Russell discloses encrypting secure content to be delivered however, Russell does not explicitly teach retrieving at the first server machine a user key permitting access to an encrypted header of the secured item.

En-Seung discloses, retrieving at a server machine a user key permitting access to an encrypted header of the secured item (See Fig. 19 and also Column 3, lines 14-32).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access information in a header and encrypt the header with a user key as in En-Seung in the system of Russell. One of ordinary skill in the art would have been motivated to do this because the system would provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information (See Column 2, lines 55-57).

En-Seung discloses an encrypted header with a user key however; he does not explicitly disclose that the encrypted header including access rules for the secured item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0066-0068).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access information of Russell in a header of secure item as taught by the combined system of Russell and En-Seung because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 21 and 35**, Russell discloses method and corresponding computer program for providing access management through use of a distributed network of server machines (see, Fig. 1), said method comprising the acts of:

(a) receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine (see, page 24, lines 2-7);

(b) authenticating a user of the client machine (see, Page 11, lines 30-31);

(c) authenticating the first client machine (See, Page 25, lines 6-14);

(d) upon successful authenticating in step (b) and (c), retrieving access rules for the secure item (see, Page 25, lines 23-30);

(e) retrieving access privileges associated with the user (see, Page 25, lines 23-30);

(f) determining whether the user is permitted to gain access to the secure item via the first server machine based on the access privileges and access rules when said authenticating (b) and (c) are successful (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13);

(g) permitting access to the secure item via the first server machine when said determining (t) determines that the user is permitted to gain access to the secure item via the first server machine (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13); and

(h) preventing access to the secure item via the first server machine when said determining (t') determines that the user is not permitted to gain access to the secure item via the first server machine (see Page 26, lines 7-9).

Russell discloses encrypting secure content to be delivered however, Russell does not explicitly teach retrieving at the first server machine a user key permitting access to an encrypted header of the secured item.

En-Seung discloses, retrieving at a server machine a user key permitting access to an encrypted header of the secured item (See Fig. 19 and also Column 3, lines 14-32).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access information in a header and encrypt the header with a user key as in En-Seung in the system of Russell. One of ordinary skill in the art would have been motivated to do this because the system would provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information (See Column 2, lines 55-57).

En-Seung discloses an encrypted header with a user key however; he does not explicitly disclose that the encrypted header including access rules for the secured item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0066-0068).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access information of Russell in a header of

secure item as taught by the combined system of Russell and En-Seung because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 2**, the rejection of claim 1 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein said determining permitting (e) comprises: (el) obtaining access privileges associated with the user to determine at least permitted locations for the user; and (e2) determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 3**, the rejection of claim 1 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein, when permitted by said permitting (e), allowing access to the secure item from the first location via the first client machine and the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 4**, the rejection of claim 1 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein, when permitted by said permitting (f), allowing access to the secure item from the first location via the first client

machine and the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claims 5 and 22**, the rejections of claims 1 and 21 are incorporated and the combination of Russell, En-Seung and Richards further discloses (h) preventing access to the secure item via any of the server machines other than the first server machine when permitting (f) permits the user to gain access to the secure item from the first location (see Russell, Page 29, lines 1-4).

Regarding **Claims 6 and 23**, the rejection of claims 1 and 21 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein said permitting (e) comprises determining whether the user is permitted to gain access to the secure item via the first client machine and the first server machine, and wherein said permitting (f) operates to permit the user to gain access to the secure item via the first client machine and the first server machine when said permitting (e) determines that the user is permitted to gain access to the secure item via both the first client machine and the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 24**, the rejections of claim 23 is incorporated and the combination of Russell, En-Seung and Richards further discloses (i) preventing access to the secure item via any of the server machines other than the first server machine when said determining (f) determines that the user is permitted to gain access to the secure item from the first location (see Page 29, lines 1-4).

Regarding **Claim 7**, the rejection of claim 1 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein said permitting (e) comprises determining whether the user is permitted to gain access to the secure item via the first server machine, and wherein said permitting (f) operates to permit the user to gain access to the secure item via the first server machine when said permitting (e) determines that the user is permitted to gain access to the secure item via the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 8**, the rejection of claim 1 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein said permitting (e) comprises determining whether the user is permitted to gain access to the secure item via the first client machine, and wherein said permitting (f) operates to permit the user to gain access to the secure item via the first client machine when said permitting (e) determines that the user is permitted to gain access to the secure item via the first client machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 9**, the rejection of claim 1 is incorporated and the combination of Russell, En-Seung and Richards further discloses (h) preventing the user from gaining access to the secure item via any of the server machines other than the first server machine when said determining permitting (e) determines that the user is permitted to gain access to the secure item from the first location (see Page 29, lines 1-4).

Regarding **Claims 10 and 25**, rejections of claims 9 and 24 are incorporated and the combination of Russell, En-Seung and Richards further discloses

wherein said preventing (h) of the user to gain access to the secure item via any of the other server machines comprises reconfiguring at least any of the other server machines that previously permitted the user to gain access to the secure item therethrough (see, Russell, Page 25, line 22- Page 26, line 2).

Regarding **Claims 11 and 26**, the rejections of claims 10 and 25 are incorporated and the combination of Russell, En-Seung and Richards further discloses said permitting (f) of the user to gain access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine (see, Russell, Page 24, lines 14-22).

Regarding **Claim 12**, the rejection of claim 13 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein said permitting (e) comprises: (el) obtaining access privileges associated with the user to determine at least permitted locations for the user (see, Russell, Page 25, lines 11-14); and determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user (see, Russell, Page 25, lines 11-14).

Regarding **Claims 13 and 27**, rejections of claims 1 and 21 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein said permitting (f) of the user to gain access to the secure item via the first server machine

comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine (see, Russell, Page 24, lines 14-22).

Regarding **Claims 14 and 28**, rejections of claims 13 and 21 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein the secure item is a secured file, the secured file having a format that comprises a header including security information as to who and how access to the secure item is permitted (see, Richards, Fig. 4 and Paragraphs 0066-0068); an encrypted data portion including data of the secured file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file (see, En-Seung, See Fig. 19 and also Column 3, lines 14-32).

Regarding **Claims 15 and 29**, rejections of claims 14 and 28 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein the security information in the header of the secured file facilitates the restricted access to the secured file (see, Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claim 16**, the rejection of claim 15 is incorporated and the combination of Russell, En-Seung and Richards further discloses wherein the security information in the header of the secured file points to or includes the access rules and a file key (see, En-Seung, Fig. 19 and also Column 3, lines 14-32 as combined with Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claims 17 and 30**, rejection of claims 14, and 28 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein the

security information is encrypted with a user key associated with the user (see, En-Seung, Fig. 19 and also Column 3, lines 14-32).

Regarding **Claims 18 and 31**, rejections of claims 14 and 28 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein the security information includes the file key and access rules to the restricted access to the secured file (see, En-Seung, Fig. 19 and also Column 3, lines 14-32 as combined with Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claims 19 and 32**, rejections of claims 18 and 28 are incorporated and the combination of Russell, En-Seung and Richards further discloses wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules (see, En-Seung, Fig. 19 and also Column 3, lines 14-32 as combined with Richards, Fig. 4 and Paragraphs 0066-0068).

Claims 20 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell in view of En-Seung and Richards and further in view of Brown et al. (US 2003/0050919 A1), hereinafter "Brown".

Regarding **Claims 20 and 33**, rejections of claims 18 and 31 are incorporated and the combination of Russell, En-Seung and Richards does not explicitly disclose access rules expressed in a markup language.

However, Brown discloses access rules expressed in a markup language (see, Fig. 5A and Paragraph 0052).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to express the access rules of the combined system of Russell, En-Seung and Richards in a markup language as taught by Brown because XML is a text-based and platform independent markup language, as a result distributor server would be able to enforce and distribute the content with policies to all client having any type of operating system platform.

Claims 36-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell in view of Richards.

Regarding **Claim 36**, Russell discloses an access control system that restricts access to a secure item (see, Fig. 1), said system comprising:

a central server having a server module that provides overall access control (see, page 16, lines 18-23); and

a plurality of local servers, each of said servers including a local module that provides local access control (see, Page 24, lines 14-22),

wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors (see, Page 16, lines 18-23), and

permitted to access the secure item through one or more of said local servers, is only able to access the secure item using only a single one of said local servers or the central server such that the given requestor is only permitted to access the secure item through at most one of said local servers at a time (see, Page 24, 14-22).

Russell discloses controlling access to a secure file, however the access control information is not stored in the header of the secure file therefore Russell does not explicitly discloses that a given requester is permitted to access a secure item based on information stored in an encrypted header of a secure item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on information stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0066-0068).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access information of Russell in a header of secure item as taught by Richards because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 37**, the rejection of claim 36 is incorporated and the combination of Russell and Richards further discloses wherein said access control system couples to an enterprise network to restrict access to the secure item, which comprises a secured file, stored therein (see Russell, Fig. 3).

Regarding **Claim 38**, the rejection of claim 37 is incorporated and the combination of Russell and Richards further discloses wherein the access requests are

at least primarily processed in a distributed manner by said local servers (see, Russell, Page 24, lines 14-22).

Regarding **Claim 39**, the rejection of claim 38 is incorporated and the combination of Russell and Richards further discloses wherein when the access requests are processed by said local servers, the requestors gain access to the secured files without having to access said central server (see, Russell, Page 24, lines 14-22).

Regarding **Claim 40**, the rejection of claim 37 is incorporated and the combination of Russell and Richards further discloses wherein the local module is a copy of the server module so any of the local modules can operate independent operate independently of said central server and other of said local servers (see, Page 23, lines 19-22).

Regarding **Claim 41**, the rejection of claim 37 is incorporated and the combination of Russell and Richards further discloses wherein the local module is a subset of the server module (see, Russell, Page 18, lines 15-17).

Regarding **Claim 42**, the rejection of claim 42 is incorporated and the combination of Russell and Richards further discloses wherein access permissions for said local servers is dynamically configured to pass a requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as when the location of the requestor changes (see, Page 20, lines 16-31).

Regarding **Claim 43**, the rejection of claim 37 is incorporated and the combination of Russell and Richards further discloses wherein the secured files are secured by encryption of the secure item (see, Page 9, lines 6-7).

Regarding **Claim 44**, the rejection of claim 37 is incorporated and the combination of Russell and Richards further discloses wherein the secure item are secured by encryption (see, page 9, lines 6-7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435